Vilniaus vandenys

PATVIRTINTA
2025-11-20 Nr. VTA-I25-241

GENERALINIS DIREKTORIUS

ĮSAKYMAS
DĖL INFORMACIJOS SAUGUMO VALDYMO SISTEMOS VADOVO PATVIRTINIMO

Siekdamas užtikrinti 2024 m. spalio 18 d. įsigaliojusio atnaujinto Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsnio 4 punkto, 2024 m. lapkričio 12 d. Lietuvos Respublikos Vyriausybės nutarimu patvirtinto Kibernetinio saugumo reikalavimų aprašo nuostatų, taikomų kibernetinio saugumo esminiams subjektams ir Lietuvos standarto LST ISO/IEC 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ reikalavimų įgyvendinimą:

1. T v i r t i n u Informacijos saugumo valdymo sistemos vadovą (pridedama) (toliau – ISVS vadovas).

2. N u s t a t a u, kad už tinkamą šio įsakymo vykdymą atsakingas Veiklos atsparumo skyriaus kibernetinio saugumo vadovas, o už vykdymo kontrolę – Veiklos atsparumo skyriaus vadovas.

3. N u s t a t a u, kad visi esami ir naujai priimami Bendrovės darbuotojai privalo susipažinti su ISVS vadovu ir laikytis jame įtvirtintų nuostatų.

4. Į p a r e i g o j u struktūrinių padalinių vadovus per 20 kalendorinių dienų pasirašytinai supažindinti savo darbuotojus, kurie neturi kompiuterizuotos darbo vietos.

5. P r i p a ž į s t u netekusiu galios generalinio direktoriaus 2023 m. liepos 24 d. įsakymą Nr. VTA-I23-168 „Dėl bendrovės informacinių sistemų saugos politikos įgyvendinimo dokumentų patvirtinimo“.

6. P a v e d u Komunikacijos skyriui ISVS vadovą paskelbti Bendrovės interneto svetainėje.

Generalinis direktorius Saulius Savickas

Rengė: J. Lisauskas, el. paštas: julius.lisauskas@vv.lt
Supažindinti: visus Bendrovės darbuotojus.

INFORMACIJOS SAUGUMO VALDYMO SISTEMOS VADOVAS	
Tikslas	Apibrėžti Bendrovės informacijos saugumo valdymo sistemos (ISVS) struktūrą, principus, atsakomybes ir taikymo sritį, siekiant: • užtikrinti, kad informacijos saugumas Bendrovėje būtų valdomas sistemingai ir nuosekliai, remiantis tarptautiniu standartu ISO 27001; • apibrėžti Informacijos saugumo politikos, procedūrų, procesų ir kontrolės priemonių tarpusavio sąsajas; • užtikrinti Bendrovės informacijos konfidencialumą, vientisumą ir prieinamumą; • užtikrinti, kad Bendrovės veikloje būtų laikomasi Lietuvos Respublikos kibernetinio saugumo įstatymo, Kibernetinio saugumo reikalavimų aprašo bei Bendrovės ISVS teisės aktų reikalavimais; • nustatyti ISVS kaip neatsiejamą Bendrovės valdymo sistemos dalį, skirtą veiklos tęstinumui, rizikų mažinimui ir kibernetinio atsparumo stiprinimui.
Taikymo sritis	Šis Vadovas taikomas: • visiems Bendrovės padaliniams, darbuotojams, rangovams ir trečiųjų šalių atstovams, kurie tvarko ar turi prieigą prie Bendrovės informacijos, informacinių sistemų ar technologinės infrastruktūros; • visoms informacijos formoms – elektroninei, popierinei, žodinei ir bet kuriai kitai, kuri naudojama Bendrovės veikloje; • visiems informacijos saugumo procesams, įskaitant rizikų valdymą, prieigos kontrolę, incidentų valdymą, veiklos tęstinumo užtikrinimą, duomenų apsaugą, tiekimo grandinės saugumą, auditą ir nuolatinį tobulinimą; • tiek informacinių technologijų (IT), tiek operacinių technologijų (OT) aplinkoms, įskaitant ypatingos svarbos informacinę infrastruktūrą (YSII); • visiems Bendrovės ISVS dokumentams, kurie detalizuoja šiame ISVS vadove nustatytus principus ir reikalavimus.
Susiję teisės aktai	Bendrasis duomenų apsaugos reglamentas; Lietuvos Respublikos kibernetinio saugumo įstatymas; Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas; Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymas; Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“; Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymo Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ reikalavimai; Standartas LST EN ISO/IEC 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga – Informacijos saugumo valdymo sistemos – Reikalavimai“; Standartas LST EN ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga – Informacijos saugumo kontrolės priemonės“; UAB „Vilniaus vandenys“ informacijos saugumo politika; UAB „Vilniaus vandenys“ konfidencialios informacijos valdymo politika; UAB „Vilniaus vandenys“ asmens duomenų tvarkymo ir saugumo politika; UAB „Vilniaus vandenys“ rizikų valdymo politika; UAB „Vilniaus vandenys“ veiklos tęstinumo politika; Atitikties užtikrinimo politika.

Turinys

1. SPECIALIOSIOS SĄVOKOS IR SUTRUMPINIMAI

Bendrasis duomenų apsaugos reglamentas (toliau – BDAR)	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB.
Bendrovė	UAB “Vilniaus vandenys”.
DAP	Duomenų apsaugos pareigūnas.
ESVP	Ekstremaliųjų situacijų valdymo planas.
Ilgalaikiai neatitikties sprendimo veiksmai (*inter alia* korekcinis veiksmas)	Veiksmai, kuriuos nurodo atsakingas vadovas ir, kurie yra skirti: (i) suvaldyti, ištaisyti, pašalinti neatitiktį ir jos pasekmes ilguoju periodu; ir (ii) užtikrinti, kad neatitiktis nepasikartotų (prevenciniai veiksmai).
ISO 27001	Standartas LST EN ISO/IEC 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (aktuali redakcija).
ISO 27002	Standartas LST EN ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“ (aktuali redakcija).
ISVG	Bendrovės generalinio direktoriaus įsakymu sudaryta darbuotojų informacijos saugumo valdymo grupė, kuri vykdo ISVS dokumentuose priskirtas funkcijas.
ISVS	Informacijos saugumo valdymo sistema.
ISVS palaikymas	Tai ISVS kūrimo, diegimo, priežiūros ir nuolatinio gerinimo veiklos.
ISVS vadovas	Informacijos saugumo valdymo sistemos vadovas.
Kibernetinis incidentas	Įvykis, dėl kurio kyla pavojus saugomų, perduodamų arba tvarkomų duomenų arba

	paslaugų, teikiamų arba prieinamų per tinklų ir IS, prieinamumui, autentiškumui, vientisumui arba konfidencialumui.
Kibernetinio saugumo subjektas	Viešasis ar privatus juridinis asmuo, kuris pagal Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatas pripažintas kaip kibernetinio saugumo subjektas ir yra įtrauktas į Kibernetinių subjektų registrą.
Kibernetinio saugumo vadovas (angl. *Chief Information Security Officer, toliau – CISO*)	Už kibernetinio saugumo valdymą atsakingas Bendrovės darbuotojas arba trečiosios šalies, teikiančios paslaugas, darbuotojas.
Kontrolės priemonės	Bendrovės taikomos organizacinės ir techninės informacijos ir kibernetinio saugumo valdymo pagrindinės ir papildomos kontrolės priemonės, numatytos Bendrovės Taikomumo pareiškime.
NKSC	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.
Pagrindinės kontrolės priemonės	Kontrolės priemonės, numatytos standarto ISO 27001 A priede ir standarte ISO 27002.
Papildomos kontrolės priemonės	Kontrolės priemonės, nenumatytos standarto ISO 27001 A priede ir standarte ISO 27002, tačiau Bendrovės pasirinktos kaip būtinas tinkamai užtikrinti informacijos ir kibernetinio saugumo valdymą.
Rizika	Neplanuotų įvykių, kurie gali paveikti Bendrovės Strategijos ir tikslų pasiekimą tiek neigiamai, tiek teigiamai, galimybė. Neapibrėžtumo poveikis tikslams, nukrypimas nuo laukiamo rezultato.
Rizikų valdymo politika	Bendrovės valdybos patvirtinta UAB „Vilniaus vandenys“ rizikų valdymo politika.
Rizikų valdymo priemonių planas	Dokumentas, kuriame nurodytos tik tos Bendrovės Rizikos, kurioms yra taikomos papildomos Rizikų valdymo priemonės, nenumatytos jokiuose kituose Bendrovės dokumentuose.
Rizikų vertinimas	Procesas, kurio metu siekiama nustatyti Rizikų Poveikio, Tikimybės reikšmes bei Rizikų lygį.
Saugumo operacijų centras (toliau – SOC)	Bendrovės generalinio direktoriaus ar jo įgalioto asmens paskirta incidentų valdymo grupė / trečiosios šalies teikiama paslauga, atsakinga už žurnalinių įrašų (angl. *Logs*) ir kibernetinių incidentų valdymą.
Taikomumo pareiškimas	Vadovybės vertinamosios analizės protokolu tvirtinamas ISVS dokumentas, kuriame numatytos standarto ISO 27001 A priede aprašytos kontrolės priemonės (pagrindinės kontrolės priemonės) ir jų netaikymo išimtys bei numatytos papildomos Bendrovės taikomos kontrolės priemonės, kurios Bendrovės manymu yra svarbios, siekiant įgyvendinti Informacijos saugumo valdymo politikoje nustatytus tikslus, tinkamai valdyti informacijos saugumo rizikas ir užtikrinti ISVS palaikymą.
Tinklų ir informacinė sistema (toliau – TIS)	Elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.
Vadovybės atstovas ISVS	Asmuo, paskirtas užtikrinti ISVS įgyvendinimą, palaikymą ir tobulinimą, atitinkant ISO 27001 standarto reikalavimus.
Veiklos atkūrimo planas (angl.	Veiklos tęstinumo valdymo tvarkos aprašo pagrindu parengtas (-i) planas (-ai), kuriame

Disaster Recovery Plan, DRP).	(-iuose) numatyti detalūs kritinės veiklos (paslaugos) ir su juo susijusių informacinių išteklių atkūrimo veiksmai pagal atskirus scenarijus, jų vykdymo eiliškumas, terminai, atsakingi padaliniai ir (ar) darbuotojai.
Veiklos tęstinumo politika	Bendrovės valdybos patvirtinta UAB „Vilniaus vandenys“ veiklos tęstinumo politika.
Veiklos tęstinumo valdymo planas (angl. *Business Continuity Plan*, BCP)	Veiklos tęstinumo valdymo tvarkos aprašo pagrindu parengtas (-i) planas (-ai), kuriame (-iuose) detalizuojama kritinės veiklos (paslaugos) ir su juo susijusių informacinių išteklių Veiklos tęstinumo strategija ir pasirengimo užtikrinti Veiklos tęstinumo valdymo priemonės, už jų įgyvendinimą atsakingi padaliniai ir (ar) darbuotojai, aprašyta esminė informacija apie kritinę veiklą (paslaugą) ir su juo susijusius informacinius išteklius, kuriems atstatyti parengtas veiklos tęstinumo valdymo planas.
VVA	Vadovybės vertinamoji analizė – periodiškai vykdomas procesas, kurio metu vadovybė įvertina vadybos sistemų tinkamumą, veiksmingumą ir galimybes tobulinti.

2. BENDROSIOS NUOSTATOS

2.1 ISVS vadovas yra pagrindinis Bendrovėje įdiegtos ir palaikomos ISVS, atitinkančios ISO 27001 reikalavimus, dokumentas, skirtas nustatyti Bendrovėje įdiegtos ir palaikomos ISVS apimtis ir taikymo sritį, numatyti ISVS sudarančių dokumentų sąrašą, nustatyti ISVS palaikymui skirtą organizacinę ir funkcinę struktūrą, aprašyti esminius ISVS procesus ir jų rezultatus.

2.2 ISVS vadovas taikomas visiems Bendrovės veiklos procesams, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo ir apima žodinę bei rašytinę informaciją, informacines sistemas, kompiuterių tinklus, fizinę aplinką, darbuotojus, susijusias šalis, partnerius, rangovus, ar kitus Bendrovėje dirbančius asmenis, įskaitant darbuotojus, dirbančius trečiosioms šalims, teisėtai tvarkančius Bendrovės informaciją.

2.3 Kitos šiame ISVS vadove naudojamos sąvokos yra suprantamos taip, kaip jos pateiktos Lietuvos Respublikos kibernetinio saugumo įstatyme ir jo įgyvendinimą reglamentuojančiuose poįstatyminiuose teisės aktuose, Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatyme, taip pat standartuose ISO 27001 ir ISO 27002.

3. INFORMACIJOS IR KIBERNETINIO SAUGUMO VALDYMO PRINCIPAI

3.1 Informacija – tai strategiškai svarbus Bendrovės veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, sugadinimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti Bendrovės kritinių veiklų (paslaugų) sutrikimą. Atsižvelgiant į tai, šis ISVS vadovas nustato pagrindines gaires, kuriomis, siekiant apsaugoti Bendrovės ir jos klientų informaciją, privalo vadovautis visi Bendrovės darbuotojai ir kitos susijusios šalys, veikiančios Bendrovės veiklos procesuose (paslaugose), kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.

3.2 Bendrovėje informacijos saugumas grindžiamas šiais kibernetinio saugumo principais:

3.2.1 Kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

3.2.2 Kibernetinio saugumo rizikos valdymo – taikomos kibernetinio saugumo rizikos valdymo priemonės turi užtikrinti Bendrovės reguliariai įvertinamos rizikos suvaldymą;

3.2.3 Kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti Bendrovės veiklos labiau, negu tai būtina kibernetiniam saugumui užtikrinti. Rizikos valdymo priemonės parenkamos įvertinus jų ekonominį naudingumą ir priimtiną riziką, kurią Bendrovė sutinka prisiimti, atsižvelgiant į veiklos kontekstą bei kritinės veiklos tęstinumo poreikius;

3.2.4 Viešojo intereso viršenybės – taikomos kibernetinio saugumo rizikos valdymo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų, Bendrovės teisių ir teisėtų interesų ar neproporcingai apriboti jų laisvės;

3.2.5 Standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo rizikos valdymo priemones, Bendrovė skatinama vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais tinklų ir IS saugumo standartais ir techninėmis specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

3.2.6 **Subsidiarumo** – už TIS ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakinga Bendrovė. Srityse, kurios priklauso išimtinei Bendrovės kompetencijai, NKSC veiksmų imasi tik tada, kai tinklų ir IS ir jomis teikiamų paslaugų kibernetinio saugumo neužtikrina Bendrovė.

3.3 Rengiant informacijos ir kibernetinio saugumo valdymą reglamentuojančius vidaus teisės aktus ir užtikrinant jų reikalavimų įgyvendinimą turi būti atsižvelgiama į aukščiau nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

4. BENDROVĖS KONTEKSTO SUVOKIMAS

4.1 Bendrovė prieš įsidiegdama ISVS sistemą, atitinkančią standarto ISO 27001 reikalavimus, taip pat prieš atlikdama kasmetinį rizikos vertinimą bei esant esminiams Bendrovės veiklos pokyčiams, nustato ir peržiūri išorinius ir vidinius veiksnius, turinčius įtakos jos gebėjimui pasiekti Bendrovės valdybos patvirtintoje Informacijos saugumo politikoje nustatytus informacijos saugumo valdymo tikslus, t. y. atlieka konteksto analizę.

4.2 Bendrovei taikomi tarptautinių ir Lietuvos teisės aktų bei standartų reikalavimai, nurodyti ISVS vadovo skiltyje „Susiję teisės aktai“.

4.3 Bendrovė pagal Lietuvos Respublikos kibernetinio saugumo įstatymo reikalavimus yra kibernetinio saugumo subjektas įtrauktas į kibernetinio saugumo subjektų sąrašą priskiriant **esminio subjekto** statusą.

4.4 Bendrovei taip pat taikomi Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo reikalavimai, kurių pagrindu Bendrovė turi rengti, tikslinti ir atnaujinti ESVP bei užtikrinti tinkamą jame numatytų veiksmų ir (ar) priemonių įgyvendinimą. ISVS taikymui turi įtakos Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatymo reikalavimai, susiję su informacijos ir kibernetinio saugumo valdymu, taip pat Bendrovės ESVP dalis, susijusi su kibernetinių incidentų, dėl kurių gali susidaryti ekstremalioji situacija, valdymu.

4.5 Bendrovėje paskirtas Vadovybės atstovas ISVS, kuris atsakingas, kad laiku būtų atlikta ar atnaujinta Bendrovės konteksto analizė bei įvertinti išoriniai ir vidiniai veiksniai, turintys įtakos jos gebėjimui pasiekti Informacijos saugumo politikoje nustatytus informacijos saugumo valdymo tikslus.

5. SUINTERESUOTŲ ŠALIŲ IR JŲ POREIKIŲ SUPRATIMAS

5.1 Bendrovė prieš įsidiegdama ISVS sistemą, atitinkančią standarto ISO 27001 reikalavimus, taip pat pasikeitus išoriniams ir (arba) vidiniams aplinkos veiksniams, kurie turi įtakos Bendrovės veiklos atsparumui, nustato ir peržiūri suinteresuotų šalių bei jų poreikių ir lūkesčių, susijusių su informacijos ir kibernetinio saugumo valdymu, sąrašą.

5.2 Vadovybės atstovas ISVS yra atsakingas, kad laiku, bet ne rečiau kaip kartą per metus būtų parengtas ir atnaujintas suinteresuotų šalių bei jų poreikių ir lūkesčių, susijusių su informacijos ir kibernetinio saugumo valdymu, sąrašas, taip pat įvertinta, kurie iš suinteresuotų šalių reikalavimų bus tenkinami taikant ISVS. Vadovybės atstovas ISVS per 20 (dvidešimt) darbo dienų nuo šio ISVS vadovo patvirtinimo dienos, vadovaudamasis Bendrovės valdybos patvirtinta Suinteresuotų šalių santykių valdymo politika, parengia suinteresuotų šalių bei jų poreikių ir lūkesčių, susijusių su informacijos ir kibernetinio saugumo valdymu, sąrašą, užpildydamas šio ISVS vadovo 1 priede pateiktą Suinteresuotų šalių bei jų poreikių ir lūkesčių sąrašo formą.

6. INFORMACIJOS SAUGUMO VALDYMO SISTEMOS TAIKYMO SRITIS

6.1 Bendrovės ISVS taikymo sritis nustatoma ir prireikus keičiama atsižvelgiant į vidaus ir išorės veiksnius (konteksto analizę) bei suinteresuotų šalių poreikius ir lūkesčius. ISVS taikymo sritį, apsvarsčius ISVG susirinkime ir (arba) VVA, nustato ir prireikus keičia Bendrovės generalinis direktorius.

6.2 Patvirtindamas šį ISVS vadovą, Bendrovės generalinis direktorius nustato tokią ISVS taikymo sritį, apimančią visą Bendrovės veiklą: **„Vandens išgavimas, paruošimas ir tiekimas. Nuotekų surinkimas ir valymas. Su tuo susijusios papildomos komercinės paslaugos, infrastruktūros ir kiti projektai“**.

6.3 ISVS palaikymui naudojamos pagrindinės ir papildomas kontrolės priemonės ir jų išimtys pagal standartų ISO27001 ir ISO 27002 reikalavimus nustatomos ir prireikus keičiamos Taikomumo pareiškime, atsižvelgiant į patvirtintą Bendrovės ISVS taikymo sritį.

6.4 Vadovybės atstovas ISVS yra atsakingas, kad laiku būtų atnaujinta ISVS taikymo sritis ir Taikomumo pareiškimas.

7. INFORMACIJOS SAUGUMO VALDYMO SISTEMA

7.1 Informacijos saugumo politikoje yra numatyti informacijos saugumo valdymo tikslai ir Bendrovės vadovybės įsipareigojimai skirti reikiamus išteklius šiems tikslams pasiekti.

7.2 Informacijos saugumo politika taip pat yra viešinama Bendrovės tinklalapyje.

7.3 Informacijos saugumo politikos tikslams detalizuoti yra sudaromi ir ISVG peržiūros posėdžio metu tvirtinami einamųjų metų Informacijos saugumo valdymo tikslai ir jų stebėjimo kriterijai, kurie planuojami ir stebimi ISVS veiksmingumo stebėsenos ir vertinimo tvarkos aprašo nustatyta tvarka. Einamųjų metų Informacijos saugumo valdymo tikslai turi būti suderinti su Informacijos saugumo politikoje nustatytais tikslais ir Bendrovės strateginiais tikslais. Einamųjų metų Informacijos saugumo valdymo tikslų įgyvendinimui turi būti skirti tam reikalingi ištekliai.

7.4 Bendrovėje įdiegta ir palaikoma ISVS, siekiant įgyvendinti Bendrovės informacijos saugumo politikoje nustatytus tikslus bei užtikrinti tarptautinių ir Lietuvos Respublikos teisės aktų, reglamentuojančių informacijos ir kibernetinio saugumo valdymą bei Lietuvos standartų reikalavimus, o taip pat Bendrovės prisiimtus sutartinius ir kitus įsipareigojimus bei suinteresuotų šalių poreikius ir lūkesčius, susijusius su informacijos ir kibernetinio saugumo valdymu.

7.5 ISVS – tai Informacijos saugumo politikos įgyvendinimą reglamentuojančių ISVS politikų, tvarkos aprašų, Taikomumo pareiškime ir kituose ISVS dokumentuose numatytų kontrolės priemonių ir už jų įgyvendinimą atsakingų Bendrovės padalinių ir darbuotojų atsakomybių ir funkcijų, visuma, kuri yra detalizuota šiame ISVS vadove ir kituose Bendrovės vidaus teisės aktuose, reglamentuojančiuose informacijos ir kibernetinio saugumo valdymą bei ISVS dokumentų įgyvendinimą, kurių sąrašas pateiktas šio ISVS vadovo 2 priede.

7.6 Visi esami ir naujai priimami Bendrovės darbuotojai, kurių darbo funkcijoms atlikti būtina prieiga prie Bendrovės TIS, Bendrovėje nustatyta tvarka privalo susipažinti, vadovaujantis „būtina žinoti" principu, su Informacijos saugumo politika ir kitais ISVS dokumentais, numatytais šio ISVS vadovo 2 priede, bei įsipareigoja laikytis jų nuostatų.

7.7 Trečiosios šalys su ISVS dokumentais, numatytais šio ISVS vadovo 2 priede, yra supažindinamos pasirašytinai pagal poreikį. Bendrovė siekdama mažinti galimas informacijos ir kibernetinio saugumo rizikas tiekimo grandinėje tinklų, duomenų centrų (debesijos) ir IS projektavimo, kūrimo, diegimo, priežiūros, vystymo ir (ar) modernizavimo ir kitiems paslaugų teikėjams (įskaitant subtiekėjams) turi nustatyti su informacijos ir kibernetinio saugumo valdymu susijusius reikalavimus pagal Kibernetinio saugumo, susijusio su trečiųjų šalių teikiamomis paslaugomis ar parduodamomis prekėmis, valdymo tvarkos aprašą ir juos numatyti tokių paslaugų ir prekių viešųjų pirkimų sutarčių sąlygose.

7.8 ISVS vadovo 2 priede nurodytų ISVS dokumentų reikalavimų privalo laikytis visi Bendrovės darbuotojai ir, pagal poreikį, trečiosios šalys.

8. INFORMACIJOS SAUGUMO VALDYMO SISTEMOS PALAIKYMUI SKIRTA ORGANIZACINĖ IR FUNKCINĖ STRUKTŪRA

8.1 Informacijos ir kibernetinio saugumo valdymui bei ISVS palaikymui sudaryta organizacinė ir funkcinė Bendrovės padalinių ir atsakingų darbuotojų, kurių funkcijos ir atsakomybės pateiktos žemiau, struktūra.

8.2 Bendrovės valdybos funkcijos ir atsakomybės numatytos Valdybos darbo reglamente.

8.3 Bendrovės Audito, rizikų ir tvarumo komiteto funkcijos ir atsakomybės numatytos Audito, rizikų ir tvarumo komiteto veiklos nuostatuose.

8.4 Bendrovės generalinis direktorius ar jo įgaliotas asmuo turi paskirti ir (arba) sudaryti:

8.4.1 ISVG;

8.4.2 Vadovybės atstovą ISVS;

8.4.3 CISO ir (arba) saugos įgaliotinį, apie jų paskyrimą Bendrovė privalo informuoti NKSC, pateikiant jo (jų) kontaktinę informaciją į NKSC administruojamą Kibernetinių subjektų informacinę sistemą (toliau – KSIS), ir Bendrovės darbuotojus. Bendrovei leidžiama iš paslaugų teikėjo (-ų) įsigyti CISO ir (arba) saugos įgaliotinio paslaugas, kurias teikiant būtų vykdomos CISO ir (arba) saugos įgaliotiniui priskirtos funkcijos;

8.4.4 Kibernetinės saugos ekspertą;

8.4.5 IS administratorių (-ius);

8.4.6 Rizikų valdymo vadovą;

8.4.7 DAP;

8.4.8 Fizinės saugos įgaliotinį;

8.4.9 SOC;

8.4.10 Veiklos tęstinumo koordinatorių;

8.4.11 Veiklos atkūrimo grupę (-es).

8.5 Bendrovės generalinio direktoriaus, Vidaus audito skyriaus ir Informacijos saugumo dalyvių, nurodytų 8.4.1 – 8.4.11 papunkčiuose, funkcijos apibrėžtos Informacijos saugumo politikoje, kituose ISVS dokumentuose ir pareigybių aprašymuose.

8.6 Esant poreikiui, Bendrovės generalinis direktorius ar jo įgaliotas asmuo gali sudaryti ir kitas informacijos ir kibernetinio saugumo valdymui bei ISVS palaikymui skirtas darbo grupes, taip pat šias funkcijas pavesti vykdyti kitiems Bendrovės darbuotojams.

8.7 Bendrovės generalinis direktorius ar jo įgaliotas asmuo, prieš Bendrovės darbuotojui pavesdamas vykdyti su informacijos ir kibernetinio saugumo valdymu bei ISVS palaikymu susijusias funkcijas ar įtraukdamas jį į atitinkamą darbo grupę, turi įsitikinti, kad šis darbuotojas turi tarptautiniuose ir Lietuvos teisės aktuose bei standartuose, taip pat ISVS dokumentuose tokioms pozicijoms nustatytus minimalius kompetencijos reikalavimus.

9. INFORMACIJOS SAUGUMO RIZIKOS VALDYMO ORGANIZAVIMAS

9.1 Informacijos saugumo valdymas Bendrovėje yra pagrįstas informacijos saugumo rizikos vertinimu ir rizikos valdymo priemonių įgyvendinimu. Informacijos saugumo rizikos vertinimas sudaro sąlygas, kad informacijos ir kibernetinio saugumo valdymo priemonės, taikomos Bendrovės veikloje, atitiktų pagrindinius Informacijos saugumo politikoje numatytus tikslus.

9.2 Informacijos saugumo rizikos valdymas Bendrovėje yra įgyvendinamas, vadovaujantis Bendrovės valdybos patvirtinta Rizikų valdymo politika ir Rizikos valdymo tvarkos aprašu.

9.3 Informacijos saugumo rizikų vertinamas atliekamas ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui.

9.4 Atlikus informacijos saugumo rizikos vertinimą, nepriimtinoms rizikoms valdyti rengiamas ir Bendrovės valdybos tvirtinamas Rizikų valdymo priemonių planas, kuriame numatoma rizikos valdymo strategija (būdas), parenkamos proporcingos rizikos valdymo priemonės, planuojamas jų įgyvendinimas, paskiriami atsakingi asmenys ir nustatomi šių priemonių veiksmingumo vertinimo kriterijai, kurie yra įtraukiami į ISVS stebėjimo planą.

9.5 Bendrovės Taikomumo pareiškime numatytos kontrolės priemonės turi būti planuojamos, kuriamos, diegiamos, naudojamos ir prižiūrimos, atsižvelgiant į atliktus Rizikos vertinimų rezultatus.

10. VEIKLOS TĘSTINUMO VALDYMO ORGANIZAVIMAS

10.1 Bendrovės veiklos tęstinumo valdymas Bendrovėje yra įgyvendinamas vadovaujantis, Bendrovės valdybos patvirtinta Veiklos tęstinumo politika ir Veiklos tęstinumo valdymo tvarkos aprašu.

10.2 Bendrovės veiklos tęstinumo valdymas, įvykus kibernetiniam incidentui, yra užtikrinamas Kibernetinių incidentų valdymo plane nustatyta tvarka.

10.3 Bendrovės veiklos tęstinumo valdymas, įvykus įvykiui, ekstremaliajam įvykiui, ypatingam įvykiui ar ekstremaliajai situacijai, yra užtikrinamas Bendrovės ESVP nustatyta tvarka.

10.4 Bendrovės ekstremaliųjų situacijų operacijų centro vadovas turi užtikrinti, kad Bendrovė būtų tinkamai pasirengusi veiklos tęstinumo valdymui įvykus kibernetiniam incidentui, taip pat, kad būtų parengti ir laiku atnaujinti Veiklos tęstinumo valdymo planai ir Veiklos atkūrimo planai bei laiku išbandomi Veiklos atkūrimo planai.

10.5 Veiklos atkūrimo valdymo grupės vadovai turi užtikrinti, kad tinkamai būtų parengti ir atnaujinti Veiklos atkūrimo planai bei laiku išbandomi Veiklos atkūrimo planai, o Veiklos atkūrimo planų išbandymo ataskaitos parengtos ir pateiktos Vadovybės atstovui ISVS pagal Veiklos tęstinumo valdymo tvarkos aprašą.

11. KVALIFIKACIJOS KĖLIMO IR KOMPETENCIJOS PALAIKYMO ORGANIZAVIMAS

11.1 Bendrovės generalinis direktorius ar jo įgaliotas asmuo, atsižvelgdamas į rizikos vertinimo rezultatus, nustatytas neatitiktis ir suplanuotus ISVS gerinimo veiksmus bei atsakingų Bendrovės darbuotojų poreikius, užtikrina tinkamą atsakingų darbuotojų kvalifikacijos kėlimą ir kompetencijos palaikymą informacijos ir kibernetinio saugumo valdymo srityje. Mokymų organizavimas aprašytas Darbuotojų pareigų, susijusių su kibernetiniu saugumu, tvarkos apraše.

11.2 Žmonių ir kultūros skyrius Bendrovėje nustatyta tvarka naujai priimtus darbuotojus turi supažindinti su Informacijos saugumo politika (visus darbuotojus) ir kitais ISVS dokumentais (atsižvelgiant į pareigybines užduotis bei “būtina žinoti” principą) bei pateikti pasirašyti Įsipareigojimą neatskleisti konfidencialios informacijos (Konfidencialios informacijos valdymo taisyklių 2 priedas). Darbuotojai raštiškai patvirtina, kad susipažino su Informacijos saugumo politika ir kitais ISVS dokumentais bei įsipareigoja laikytis jų nuostatų.

12. KOMUNIKAVIMO ORGANIZAVIMAS

12.1 Bendrovėje nustatoma vidinė ir išorinė su ISVS susijusi komunikacija, įskaitant jos: turinį (komunikacijos turinio strategija), laiką (kada komunikuoti), adresatus (kam komunikuoti), būdus (kokiais kanalais komunikuoti), vykdytojus (kas komunikuos), kalbas (kokiomis kalbomis komunikuoti).

12.2 Bendrovėje planuojant ir rengiant atskirus pranešimus, susijusius su Informacijos saugumo politika, ISVS ir (arba) informacijos ir kibernetinio saugumo incidentais, jų turinys ir paskelbimo laikas turi būti suderinti su Vadovybės atstovu ISVS.

12.3 Vadovybės atstovas ISVS konsultuoja Bendrovės generalinį direktorių, tarnybų direktorius, Komunikacijos vadovą ir struktūrinių padalinių vadovus, o jų nesant – atsakingus darbuotojus, jiems bendraujant su žiniasklaida ISVS klausimais.

12.4 Už vidinę komunikaciją, susijusią su ISVS, yra atsakingas Vadovybės atstovas ISVS ir (arba) CISO, kuris savarankiškai pasirenka ir planuoja, kokias žinutes (pranešimus ir pan.), kam, kuriuo laiku ir kokiomis priemonėmis teikia Bendrovės darbuotojams. Įgyvendindamas vidinę komunikaciją, susijusią su ISVS, Vadovybės atstovas ISVS ir (arba) CISO bendradarbiauja su Komunikacijos skyriaus Vidine komunikacijos partnere.

12.5 Vadovybės atstovas ISVS, CISO, DAP arba jų deleguoti kiti Bendrovės darbuotojai Lietuvos Respublikos teisės aktų nustatyta tvarka ir terminais bei būdu užtikrina išorinę komunikaciją su kontroliuojančiomis institucijomis – NKSC, Valstybine duomenų apsaugos inspekcija ir Policija, susijusią su informacijos ir kibernetinio saugumo incidentais.

12.6 Vadovybės atstovas ISVS ir (arba) CISO arba jų deleguoti kiti Bendrovės darbuotojai sudarytų sutarčių pagrindu užtikrina išorinę komunikaciją su išorės paslaugų teikėjų atsakingais darbuotojais, susijusią su ISVS palaikymu bei informacijos ir kibernetinio saugumo įvykiais ir incidentais.

12.7 Vadovybės atstovas ISVS ir (arba) CISO turi užtikrinti, kad į viešųjų pirkimų dokumentus būtų perkeltos būtinosios į sutartis įtraukti informacijos ir kibernetinio saugumo nuostatos. Vadovaujamasi Viešųjų pirkimų vykdymo tvarkos aprašu ir Kibernetinio saugumo, susijusio su trečiųjų šalių teikiamomis paslaugomis ar parduodamomis prekėmis, valdymo tvarkos aprašu.

13. ISVS PLANAVIMAS, ĮGYVENDINIMAS, STEBĖJIMAS IR ĮGYVENDINIMO KONTROLĖ

13.1 Bendrovė planuoja, įgyvendina, analizuodama vertina ir valdo ISVS procesus ir įgyvendina informacijos saugumo rizikos valdymą, atlikdama šiuos veiksmus:

13.1.1 laiku ir tinkamai planuodama ISVS procesų, įskaitant rizikos vertinimą, taip pat Taikomumo pareiškime numatytų kontrolės priemonių ir rizikos valdymo priemonių bei neatitikčių šalinimo ir ISVS gerinimo veiksmų įgyvendinimą;

13.1.2 ISVS procesus, įskaitant rizikos vertinimą, taip pat Taikomumo pareiškime numatytas kontrolės priemones ir rizikos valdymo priemones bei neatitikčių šalinimo ir ISVS gerinimo veiksmus įgyvendindama šiame ISVS vadove ir ISVS dokumentuose nustatyta tvarka ir terminais;

13.1.3 stebėdama ir matuodama ISVS stebėjimo plane numatytus ISVS procesų, įskaitant rizikos vertinimo, taip pat Taikomumo pareiškime numatytų kontrolės priemonių ir rizikos valdymo priemonių bei neatitikčių šalinimo ir ISVS gerinimo veiksmų įgyvendinimo ir efektyvumo matavimo kriterijus;

13.1.4 saugodama tokią dokumentuotą informaciją, kurios reikia siekiant įsitikinti, kad ISVS sudarantys procesai, Taikomumo pareiškime numatytos kontrolės priemonės ir rizikos valdymo priemonės bei neatitikčių šalinimo ir ISVS gerinimo veiksmai buvo atlikti taip, kaip planuota.

13.2 Į ISVS sudarančius procesus yra įtraukti Taikomumo pareiškime numatytų kontrolės priemonių įgyvendinimo procesai.

13.3 Taikomumo pareiškime numatytų kontrolės priemonių įgyvendinimo procesai yra numatyti atitinkamuose ISVS dokumentuose, kurie yra tvirtinami Bendrovės generalinio direktoriaus įsakymais.

13.4 Vadovybės atstovas ISVS ir (arba) CISO turi periodiškai, kartą į metus, peržiūrėti ISVS dokumentus ir pagal poreikį juos atnaujinti.

13.5 Pranešimai apie informacijos ir kibernetinio saugumo įvykius ir incidentus yra teikiami Kibernetinių incidentų valdymo plano nustatyta tvarka, terminais bei būdais.

13.6 Bendrovės ISVS procesų, įskaitant rizikos vertinimo, taip pat Taikomumo pareiškime numatytų kontrolės priemonių ir rizikos valdymo priemonių bei neatitikčių šalinimo ir ISVS gerinimo veiksmų įgyvendinimo ir efektyvumo stebėjimas, matavimai, analizė ir įvertinimas vykdomi pagal ISVS veiksmingumo stebėsenos ir vertinimo tvarkos aprašą.

14. ISVS VIDAUS AUDITAS, ATITKTIES VERTINIMAS IR NEATITIKČIŲ ŠALINIMAS

14.1 ISVS vidaus auditas yra atliekamas ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui, vadovaujantis Bendrovės valdybos tvirtinamu Vidaus audito veiklos tvarkos aprašu.

14.2 Vidaus auditą Bendrovėje atlieka Bendrovės Vidaus audito skyrius, arba, esant poreikiui, vidaus auditas gali būti atliekamas pasitelkiant išorės auditorius – trečiąją šalį.

14.3 Ne rečiau kaip kartą per metus arba įvykus reikšmingiems Bendrovės pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui, Vadovybės atstovas ISVS ir (arba) CISO atlieka Atitikties vertinimą pagal Atitikties vertinimo tvarkos aprašą. Esant poreikiui, Atitikties vertinimas gali būti atliekamas pasitelkiant išorės vertintojus – trečiąją šalį.

14.4 Bendrovė ne rečiau kaip kartą per 3 metus privalo organizuoti Atitikties vertinimą, kurį atliktų nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti auditoriai Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka.

14.5 Už ISVS neatitikčių (esamų ir (arba) galimų ISVS reikalavimų nevykdymo) nustatymą pagal gautą informaciją, neatitikčių registravimą neatitikčių registre yra atsakingas audituojamo Bendrovės struktūrinio padalinio vadovas ir (arba) Vadovybės atstovas ISVS. Bendrovės atitinkamo skyriaus/padalinio vadovai yra atsakingi už neatitikties sprendimo plano sudarymą ir neatitikties faktinį įgyvendinimą (išsprendimą).

14.6 ISVS neatitikčių valdymas vykdomas vadovaujantis Neatitikčių valdymo tvarkos aprašu.

15. ISVS VALDYMO PERŽIŪRA IR NUOLATINIS GERINIMAS

15.1 Bendrovė nuolat gerina ISVS tinkamumą, proporcingumą ir rezultatyvumą, atlikdama ISVS stebėjimą, reaguojant į visas neatitiktis ir vykdant jų šalinimo stebėseną, atliekant rizikos vertinimą ir įgyvendinant rizikos valdymo priemones, organizuojant ISVG susirinkimus, įgyvendinant ISVS vidaus ir išorės auditų bei atitikties vertinimų rekomendacijas, atliekant ISVS valdymo peržiūrą ir įgyvendinant numatytas ISVS gerinimo priemones.

15.2 ISVG susirinkimai organizuojami ne rečiau kaip kartą į pusmetį, siekiant peržiūrėti ISVS pusmečio rezultatus, peržiūrėti ir teikti Bendrovės generaliniam direktoriui tvirtinti parengtus planus ir ISVS procesų rezultatus bei prioretizuoti ISVS veiksmus, numatytus kitam pusmečiui, o taip pat užtikrinti tinkamą ISVS palaikymą.

15.3 ISVG susirinkimus organizuoja ir jiems vadovauja Vadovybės atstovas ISVS. Bendrovės generaliniam direktoriui dalyvaujant ISVG posėdyje, jam pirmininkauja Bendrovės generalinis direktorius.

15.4 ISVG susirinkimai pagal poreikį gali būti protokoluojami. Juos protokoluoja Teisės skyriaus paskirtas darbuotojas arba Vadovybės atstovo ISVS paskirtas kitas ISVG narys.

15.5 Bendrovės valdymo peržiūra atliekama ne rečiau kaip kartą per metus pagal Vadovybės vertinamosios analizės peržiūros tvarkos aprašą.

15.6 Bendrovei nustačius, kad ISVS reikia keisti, pakeitimai atliekami planuotai, atsižvelgiant į pakeitimų tikslą ir galimas jų pasekmes, ISVS vientisumą, esamus išteklius, atsakomybės ir įgaliojimų paskirstymą ar perskirstymą bei pakeitimų įgyvendinimo tempą, mastą ir laikotarpį.

15.7 Bendrovės darbuotojai pastabas ir pasiūlymus dėl ISVS gerinimo gali teikti tiesiogiai Vadovybės atstovui ISVS (el. paštu, Teams ar tiesiogiai). Bendrovės vadovybei ISVS valdymo peržiūros metu priėmus sprendimą gerinti ISVS, Vadovybės atstovas ISVS per 10 darbo dienų nuo sprendimo priėmimo dienos turi parengti ir Bendrovės generaliniam direktoriui pateikti tvirtinti ISVS gerinimo planą, kuriame turi būti numatytos veiklos, jų įgyvendinimo terminai ir už jų įgyvendinimą atsakingi Bendrovės padaliniai ir (arba) darbuotojai.

15.8 Bendrovės darbuotojams pateikus pasiūlymus dėl ISVS gerinimo ar Vadovybės atstovui ISVS pačiam nustačius ISVS gerinimo galimybes, Vadovybės atstovui ISVS apibendrintą informaciją pateikia eiliniame ISVG posėdyje ir jame priėmus sprendimą gerinti ISVS, Vadovybės atstovas ISVS per 20 darbo dienų nuo sprendimo priėmimo dienos turi parengti ir Bendrovės generaliniam direktoriui pateikti tvirtinti ISVS gerinimo planą, kuriame turi būti numatytos veiklos, jų įgyvendinimo terminai ir už jų įgyvendinimą atsakingi Bendrovės padaliniai ir (ar) darbuotojai.

16. DOKUMENTUOTUOS INFORMACIJOS VALDYMAS

16.1 Į Bendrovės ISVS įtraukiama ir privalomai dokumentuojama tokia informacija:

16.1.1 Bendrovės darbuotojų supažindinimas su ISVS dokumentais;

16.1.2 ISVS dokumentų peržiūros ir atnaujinimo įrašai;

16.1.3 ISVS sudarančių procesų planavimo ir įgyvendinimo įrašai;
16.1.4 Rizikos vertinimo rezultatai;
16.1.5 Atitikties vertinimo rezultatai;
16.1.6 Veiklos atkūrimo planų išbandymo rezultatai;
16.1.7 įrašai apie Bendrovės organizuotus ir įgyvendintus informacijos ir kibernetinio saugumo valdymo mokymus ir (arba) šiuose mokymuose ir kituose renginiuose dalyvavusius Bendrovės darbuotojus;
16.1.8 Trečiųjų šalių pateikti dokumentai, susiję su jų prisiimtų įsipareigojimų, susijusių su informacijos ir kibernetinio saugumo valdymu, tinkamu įgyvendinimu;
16.1.9 ISVS stebėjimo rezultatai;
16.1.10 pagal poreikį ISVG posėdžių rezultatai;
16.1.11 ISVS vidaus audito rezultatai;
16.1.12 ISVS valdymo peržiūros rezultatai;
16.1.13 Neatitikčių šalinimo ir ilgalaikių neatitikčių sprendimo veiksmų (tame tarpe ir korekcinių veiksmų) įgyvendinimo rezultatai;
16.1.14 Rizikų valdymo priemonių plano įgyvendinimo rezultatai;
16.1.15 ISVS gerinimo priemonių plano įgyvendinimo rezultatai;
16.1.16 kita informacija, kurią Vadovybės atstovas ISVS laiko būtina ISVS palaikymui.

16.2 Dokumentai, susiję su ISVS, rengiami, derinami, pasirašomi ir saugomi vadovaujantis Dokumentų rengimo ir valdymo tvarkos aprašu.

17. BAIGIAMOSIOS NUOSTATOS

17.1 Bendrovės darbuotojams ir trečiosioms šalims, pažeidusiems Informacijos saugumo politikos ir kitų ISVS dokumentų reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės. Aktuali ISVS vadovo redakcija skelbiama dokumentų valdymo sistemoje ir yra prieinama visiems darbuotojams.

17.2 ISVS vadovas tvirtinamas ir keičiamas Bendrovės generalinio direktoriaus įsakymu.

17.3 Vadovybės atstovas ISVS ir (arba) CISO nuolat stebi ISO 27000 grupės standartų, tarptautinių ir Lietuvos Respublikos teisės aktų, reglamentuojančių informacijos ir kibernetinį saugumo valdymą, pasikeitimus ir, esant poreikiui, atnaujina ISVS vadovą ir kitus ISVS dokumentus.

17.4 ISVS vadovas ir kiti ISVS dokumentai peržiūrimi ne rečiau kaip kartą per metus ir pagal poreikį atnaujinami, atsižvelgiant į Vadovybės atstovo ISVS ir (arba) CISO pastabas ir (arba) gerinimo pasiūlymus, valstybėje ir Bendrovėje vykstančius pokyčius, Bendrovės valdybos, Bendrovės generalinio direktoriaus sprendimus ir kitus objektyvius veiksnius.

17.5 Už ISVS vadovo ir kitų ISVS dokumentų parengimą ir atnaujinimą, įgyvendinimo kontrolę yra atsakingas Vadovybės atstovas ISVS ir (arba) CISO, nebent ISVS dokumente numatyta kitaip.

PRIEDAI

1 priedas. Suinteresuotų šalių bei jų poreikių ir lūkesčių sąrašo forma.
2 priedas. Informacijos saugumo valdymo sistemą (ISVS) sudarančių dokumentų susipažinimo matrica.

_____

INFORMACIJOS SAUGUMO VALDYMO SISTEMĄ SUDARANČIŲ DOKUMENTŲ SUSIPAŽINIMO MATRICA

Nr.	Dokumento pavadinimas	Visi darbuotojai	Kiti pagal poreikį (nurodoma įsakymuose): Struktūrinių padalinių vadovai Darbuotojai su KDV ISVG nariai Vidaus audito skyriaus darbuotojai Vadovybės atstovas ISVS Kibernetinio saugumo vadovas ir (arba) Saugos įgaliotinis IT skyriaus darbuotojai IS administratoriai Rizikų valdymo vadovas Veiklos tęstinumo koordinatorius Duomenų apsaugos pareigūnas Kibernetinės saugos ekspertas Fizinės saugos projektų vadovas Saugumo operacijų centras (SOC) Kiti
1.	Informacijos saugumo politika	X	
2.	Konfidencialios informacijos valdymo politika	X	
3.	Asmens duomenų tvarkymo ir saugumo politika	X	
4.	Rizikų valdymo politika	X	
5.	Veiklos tęstinumo valdymo politika	X	
6.	Atitikties užtikrinimo politika	X	
7.	Fizinės ir veiklos apsaugos reglamentas	X	
8.	Bendrovės informacinių sistemų duomenų saugos nuostatai	X	
9.	Informacijos saugumo valdymo sistemos vadovas	X	
10.	Taikomumo pareiškimas		X
11.	Kibernetinių incidentų valdymo planas	X	
12.	Elektroninių duomenų valdymo tvarkos aprašas		X
13.	Prieigų valdymo tvarkos aprašas	X	
14.	Techninių reikalavimų įgyvendinimo ir pažeidžiamumų valdymo tvarkos aprašas		X
15.	Pataisų valdymo tvarkos aprašas		X
16.	Žurnalinių įrašų valdymo tvarkos aprašas		X

17.	Atsarginių kopijų valdymo tvarkos aprašas		X
18.	Kibernetinio saugumo, susijusio su trečiųjų šalių teikiamoms paslaugomis ar parduodamomis prekėmis, valdymo tvarkos aprašas	X	
19.	Kriptografinių raktų valdymo tvarkos aprašas		X
20.	Veiklos tęstinumo valdymo tvarkos aprašas		X
21.	Rizikos valdymo tvarkos aprašas	X	
22.	Darbuotojų pareigų, susijusių su kibernetiniu saugumu, tvarkos aprašas	X	
23.	Mobiliųjų įrenginių valdymo tvarkos aprašas	X	
24.	Išorinių įrenginių naudojimo tvarkos aprašas		X
25.	Elektroninio pašto ir interneto naudojimo tvarkos aprašas	X	
26.	Saugaus informacijos teikimo tvarkos aprašas	X	
27.	Darbuotojų IT įrangos ir informacinių sistemų elektroninės informacijos naudojimosi tvarkos aprašas		X
28.	IT sistemų plėtros valdymo tvarkos aprašas		X
29.	Informacijos saugumo valdymo sistemos veiksmingumo stebėsenos ir vertinimo tvarkos aprašas		X
30.	Vidaus audito veiklos tvarkos aprašas		X
31.	Atitikties vertinimo tvarkos aprašas		X
32.	Neatitikčių valdymo tvarkos aprašas	X	
33.	Viešųjų pirkimų vykdymo tvarkos aprašas		X
34.	Projektų valdymo tvarkos aprašas		X
35.	Vadovybės vertinamosios analizės tvarkos aprašas	X	
36.	Patekimo į UAB „Vilniaus vandenys“ centrinę buveinę taisyklės		X
37.	Konfidencialios informacijos valdymo taisyklės	X	
38.	Asmens duomenų tvarkymo ir saugumo politikos įgyvendinimo taisyklės	X	
39.	Atsakingų už fizinę saugą darbuotojų sąrašas		X

_____